IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION
Case No:

TAMMY STANLEY CLONCH, on behalf of herself and all others similarly situated, Plaintiff, v. THE CHARLOTTE-MECKLENBURG HOSPITAL AUTHORITY (d/b/a ATRIUM HEALTH), Defendant.	**CLASS ACTION COMPLAINT AND JURY DEMAND**

Plaintiff Tammy Stanley Clonch ("Plaintiff" or "Clonch"), by and through her attorneys of record, upon personal knowledge as to her own acts and experiences, and upon information and belief as to all other matters, which Plaintiff believes will be supplemented and supported after a reasonable opportunity for discovery, brings this class action complaint against Defendant the Charlotte-Mecklenburg Hospital Authority (d/b/a Atrium Health) ("Atrium" or "Defendant") and alleges as follows:

INTRODUCTION

1. Plaintiff brings this class action on behalf of a Class, as defined below, against Defendant for its failure to properly secure and safeguard Plaintiff's and Class Members' protected personal information stored within Defendant's information networks and servers, including, without limitation, "protected health information" ("PHI"), [1] and "personally identifiable

[1] Protected Health Information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. *Inter alia*, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

information" ("PII"),[2] as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively, PHI and PII are also referred to therein as "Private Information").

2. Defendant is a hospital network operating approximately forty hospitals, forty-two emergency departments, fifty-eight urgent care centers, and hundreds of medical care facilities in North Carolina, South Carolina, Georgia, and Alabama.[3]

3. In the course of providing its services, Defendant acquired and collected Plaintiff's and Class Members' Private Information. Defendant knew at all times material that it was collecting, and was responsible for the security of sensitive data, including Plaintiff's and Class Members' highly confidential Private Information. This Private Information remains in the possession of Defendant, despite the fact that it was accessed by unauthorized third persons, is currently being maintained without appropriate and necessary safeguards, independent review, and oversight, and therefore remains vulnerable to additional hackers and theft.

4. Plaintiff seeks to hold Defendant responsible for the harms they caused and will continue to cause Plaintiff and other similarly situated persons by virtue of a preventable phishing-based cyberattack on Defendant's network that occurred on April 29-30, 2024 (the "Data Breach").[4]

5. As a consequence, the Private Information that Defendant was entrusted with and responsible for, was accessed. This Private Information is significantly valuable to data thieves.

---

[2] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[3] See https://cdn.atriumhealth.org/-/media/newsroom/pdfs/22-0012280-enterprise-annual-report_web-min.pdf?rev=8f8652a45fc348b98435744e131706e5 (last visited October 7, 2024).

[4] See https://atriumhealth.org/about-us/newsroom/news/phishing-email-may-have-impacted-personal-information (last visited October 7, 2024).

Plaintiff further seeks to hold Defendant responsible for not ensuring that the Private Information was maintained in a manner consistent with industry standards.

6. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information. The Data Breach occurred because Defendant maintained Class Members' Private Information in a reckless manner, and on its computer network in a condition that was vulnerable to cyber-attack.

7. As a result of the Data Breach, the Private Information belonging to Plaintiff and Class Members was lost. This Private Information included first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; driver's license or state-issued identification number; certain government or employer identifiers; bank or financial account numbers or information, including routing numbers, financial institution name, security code/PIN and/or expiration date; treatment/diagnosis, prescription, health insurance and/or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.[5]

8. Plaintiff seeks to hold Defendant responsible for not ensuring that Private Information, as defined by HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), and respecting which Defendant was duty bound to protect pursuant to the HIPAA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), was maintained in a manner consistent with industry standards, and other relevant standards.

9. HIPAA, in general, applies to healthcare providers and those health care providers that conduct certain health care transactions electronically, and HIPAA Business Associates, and sets standards for Defendant's maintenance of Plaintiff's and Class Members' Private Information, including appropriate safeguards to be maintained by organizations such as Defendant's to protect

[5] *Id*.

the privacy of patient health information, while setting limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

10. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a HIPAA Business Associate. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI. HIPAA provides the standard of procedure by which a medical provider must operate when collecting, storing, and maintaining the confidentiality of Private Information.

11. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant knowingly assumed legal and equitable duties to those individuals, including those arising from common law principles.

12. The risk of cyber-attack was well-known to Defendant and it was continuously on notice at all times material that its failure to take steps necessary to secure the Private Information from a risk of cyber-attack and unauthorized access left that information and property in a dangerous condition that was vulnerable to theft and misuse.

13. Although Defendant knew of the cyber-attack by no later than April 29, 2024, and completed a "forensic examination" of email accounts affected by the cyber-attack on July 17, 2024, it failed to disclose the event, or otherwise provide its individual clients notice of the Data Breach until September 13, 2024.[6]

14. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to those individuals. These duties arise from state and federal statutes and regulations, as well as common law principles.

15. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take

[6] *Id*.

available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, upon information and belief, the Private Information of Plaintiff and Class Members was compromised and damaged through access by and disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future – thus entitling them to damages. In addition, Plaintiff and Class Members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiff Tammy Stanley Clonch

16. Plaintiff Clonch is, and at all relevant times was, a citizen of the state of North Carolina and a resident of North Wilkesboro.

17. Plaintiff received healthcare from Atrium Health for many years. As a condition of receiving services from Defendant, Plaintiff was required to provide Defendant with substantial and sensitive Private Information.

18. Plaintiff provided substantial Private Information, including, but not limited to, her first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; certain government or employer identifiers; driver's license or state-issued identification number; bank or financial account numbers or information, including routing numbers, financial institution name, or expiration date; treatment/diagnosis, provider name, prescription, health insurance or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.

19. Plaintiff received a letter from Defendant, dated September 13, 2024, notifying her that her information had been accessed by third party actors.

20. According to this letter, Defendant learned that an unauthorized third party gained access to Atrium's computer network between April 29-30, 2024 and the breach was discovered by Defendant on April 29, 2024. Defendant claimed that it did not determine that Plaintiff's Private Information had been affected by this incident until July 17, 2024.

21. Plaintiff takes care in protecting her Private Information from disclosure. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Faced with the risk of the unauthorized disclosure of her PII, Plaintiff is now forced to monitor her accounts for signs of fraud and identity theft and devote valuable time and resources to same.

22. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff will have to worry about when and how her sensitive information may be shared or used to her detriment.

23. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of her privacy.

Defendant Atrium

24. Defendant is a Charlotte, North Carolina-based health care provider maintaining its principal place of business at 1000 Blythe Boulevard, Charlotte, North Carolina 28203.

25. Defendant collects and requires its patients to provide Private Information in the course of providing its services.

26. By obtaining, collecting, using, and deriving benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to those persons and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and/or criminal hacking activity.

JURISDICTION AND VENUE

1. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy, exclusive of interest and costs, exceeds the sum value of $5,000,000.00, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class are citizens of states different than that of Defendant.

2. This Court has personal jurisdiction over Defendant because Defendant is authorized to conduct business within this District, is headquartered in this District, and regularly conducts business in this District.

3. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this action occurred in this District.

FACTUAL BACKGROUND

Defendant's Business Involving the Collection and Maintenance of Private Background

4. Defendant is a healthcare provider with facilities in North Carolina, South Carolina, Alabama, and Georgia.[7]

5. As part of its services, Defendant collected Private Information from its patients, including but not limited to: first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; driver's license or state-issued identification number; certain government or employer identifiers; bank or financial account numbers or information, including routing numbers, financial institution name, security code/PIN and/or expiration date; treatment/diagnosis, prescription, health insurance and/or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.[8]

[7] See https://cdn.atriumhealth.org/-/media/newsroom/pdfs/22-0012280-enterprise-annual-report_web-min.pdf?rev=8f8652a45fc348b98435744e131706e5 (last visited October 7, 2024).

[8] See https://atriumhealth.org/about-us/newsroom/news/phishing-email-may-have-impacted-personal-information (last visited October 7, 2024).

6. Defendant requires those persons receiving its services – including its patients – to provide their Private Information, which Defendant is obligated to keep confidential and private.

7. In the course of its business, Defendant acquired, collected, stored, and assured the security of, the Private Information of Plaintiff and the Class.

8. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. The information collected, acquired, and stored by Defendant included the Private Information of Plaintiff and Class Members.

9. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their Private Information.

10. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. To that end, Defendant was reposed with a legal duty created by HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

11. By obtaining, collecting, using, and storing Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure. And given the highly sensitive nature of the Private Information it possessed and the sensitivity of the medical and health services it provides, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' Private Information.

12. Defendant retains and stores this Private Information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to perform its services.

13. Defendant's failure to adequately safeguard the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

14. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation.

15. Defendant was obliged by contract, industry standards, common law, and promises and representations made to Plaintiff and Class Members, to keep their Private Information confidential and protect it from unauthorized access and disclosure.

16. Plaintiff and Class Members had a reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep the Private Information they provided confidential and secure from unauthorized access and disclosure.

17. Defendant's own Privacy Policy expressly comforts clients and their patients with the representation "We Are Required by Law" to "[m]aintain the privacy of your health information . . . ."[9]

The Data Breach

18. On April 29-30, 2024, an unauthorized party gained access to the email accounts of certain employees of Defendant through what is commonly known as a "phishing" attack. A phishing attack is a cyber-intrusion, typically using a phone call, text, or email designed to appear that it is from a trustworthy source but is, in fact, designed to capture information for use by unauthorized third parties. Through this phishing attack, an unauthorized third party was able to gain account login information for certain email accounts operated by employees of Defendant. By doing so, hackers were able to access Private Information of Plaintiff and the Class that was

[9] See https://atriumhealth.org/for-patients-visitors/privacy/english (last visited October 7, 2024).

included in the data of compromised email accounts. Defendant discovered this unauthorized access on April 29, 2024.

19. Defendant was aware that it maintained substantial Private Information of its patients, including, but not limited to names, first and/or last name; middle initial; street address, email address and/or phone number(s); Social Security number; date of birth; medical record number; driver's license or state-issued identification number; certain government or employer identifiers; bank or financial account numbers or information, including routing numbers, financial institution name, security code/PIN and/or expiration date; treatment/diagnosis, prescription, health insurance and/or treatment cost information; patient identification number; health insurance account or policy number(s); incidental health references; billing identification numbers; access credentials; and/or digital signatures.

20. However, despite learning of the Data Breach on April 29, 2024, and completing a forensic examination no later than July 17, 2024, it wasn't until September 13, 2024 that Defendant began informing Plaintiff and the Class that the Data Breach had compromised their Private Information by sending out data breach notice letters to individuals who were affected by the Data Breach.[10]

21. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information of numerous patients.

22. Because of Defendant's negligence and misconduct in failing to keep the accessed information confidential, the unencrypted Private Information of Plaintiff and Class Members has been expropriated by unauthorized individuals who can now exploit the PHI and PII of Plaintiff and Class Members and use it as they please.

[10] *See* https://atriumhealth.org/about-us/newsroom/news/phishing-email-may-have-impacted-personal-information (last visited July 24, 2024).

23. Plaintiff and Class Members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendant when receiving services.

24. As a consequence of Defendant's inadequate data security systems and protection, Plaintiff and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendant. Plaintiff and Class Members, understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant had not provided the necessary adequate data security in any event. Consequently, Plaintiff and Class Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendant.

Defendant's Business and Obligation to Preserve and Protect Confidentiality and Privacy

25. Defendant was entrusted with highly sensitive Private Information, including names, date of birth, medical information, and other highly sensitive PHI and PII. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects.

26. Plaintiff and Class Members are current or former patients of Defendant who obtained service(s) through Defendant.

27. Plaintiff and Class Members provided their Private Information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access, and Defendant expressly represented in its Privacy Policy that it would do so.[11]

28. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to

[11] *https://atriumhealth.org/for-patients-visitors/privacy/english* (last visited October 7, 2024).

make only authorized disclosures of this information. Plaintiff and Class Members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. In addition to obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties, and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

30. At all times material, Defendant was under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. And to that end, Defendant also had a legal duty created by contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure. Given the highly sensitive nature of the Private Information that Defendant possessed and the sensitivity of the services it provided, Defendant had a duty to safeguard, protect, and encrypt Plaintiff's and Class Members' PII.

31. By obtaining, collecting, storing, and transmitting the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

32. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

33. Defendant, via its Privacy Policy, expressly promised to maintain and protect the Private Information of Plaintiff and the Class, demonstrating an understanding of the importance of securing Private Information.

34. Defendant's failure to safeguard the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

35. Defendant was not permitted to disclose Plaintiff's and Class Members' Private Information for any reason that would apply in this situation. The disclosure of Plaintiff's and Class Members' Private Information via the Data Breach was not permitted per Defendant's own policies.

36. Defendant failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining of Plaintiff and Class Members, consequently enabling and causing the exposure of Private Information in the Data Breach.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

37. The PII of consumers, such as Plaintiff and Class Members, is valuable and has been commoditized in recent years.

38. Defendant was also aware of the significant repercussions that would result from its failure to protect Private Information and knew, or should have known, the importance of safeguarding the Private Information entrusted to themselves and of the foreseeable consequences in the event of a breach of its data security. Nonetheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

39. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

40. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud

alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

41. Even absent any adverse use, consumers suffer injury from the simple fact that Private Information has been stolen. When such sensitive information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the community.

42. Plaintiff and the other Class Members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Purchasing credit monitoring and identity theft prevention;

C. Taking trips to banks and waiting in line to verify their identities in order to restore access to compromised accounts;

D. Placing freezes and alerts with credit reporting agencies;

E. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

F. Contacting their financial institutions and closing or modifying financial accounts;

G. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

H. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

I. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

43. Moreover, Plaintiff and the other Class Members have an interest in ensuring that Defendant implements reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible by unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendant is fully secure, remains secure, and is not subject to future theft.

44. As a further direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

45. As a direct and proximate result of Defendant's wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiff's and other Class Members' Private Information, Plaintiff and all Class Members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other personal accounts—for which they are entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Defendant Was Well Aware of the Threat of Cyber Theft and Exfiltration in Healthcare Related Industries

46. As a condition of Defendant's relationships with its clients, customers, and Class Members, Defendant required that they entrust it with highly sensitive and confidential PII. Defendant, in turn, collected that information and assured consumers that it was acting to protect that PII and to prevent its disclosure.

47. Defendant could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

48. Defendant's overt negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as an entity operating in the health, pharmaceutical and services industries, Defendant was on notice that such companies are targets for data breach hackers and cyber-thieves.

49. PII, including names and social security numbers, is uniquely valuable to hackers. With these pieces of information, criminals can open new financial accounts in Class Members' names, take loans in their names, use their names to obtain medical services, obtain government benefits, file fraudulent tax returns in order to get refunds to which they are not even entitled, and numerous other assorted acts of thievery and fraud.

50. For this reason, hackers prey on companies that collect and maintain sensitive information, including medical institutions, insurers, and related entities. Companies like Defendant's have been aware of this, and the need to take adequate measures to secure their systems and information, for a number of years. In 2021 alone, approximately 330 breaches targeting healthcare providers occurred.[12] The steady growth of hacks of healthcare service providers is no surprise and can be tied to two significant factors, (1) the failure of healthcare services providers, like Defendant's, to adequately protect patient data and (2) the substantial value of the sensitive PII entrusted to healthcare service providers.

51. In the context of data breaches, healthcare is "by far the most affected industry sector."[13] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[14]

---

12 ITRC_2021_Data_Breach_Report.pdf (idtheftcenter.org) at 6. (last visited on October 7, 2024).

13 Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited October 7, 2024).

14 *Id.*

52. In 2021, 1,862 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, an increase of 68% over 2020 and a 23% increase over the previous all-time high.[15] These data breaches exposed the sensitive data of approximately 294 million people. *Id.*

53. Companies like Defendant's are well aware of the risk that data breaches pose to consumers, especially because both the size of its customer base and the fact that the PII that it collects and maintains is profoundly valuable to hackers.

54. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII.

55. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiff and Class Members.

56. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

57. Because Defendant failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Upon information and belief, Defendant still maintains the PII of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Representative Plaintiff's and Class Members' PII remain at risk of subsequent data breaches.

58. In addition to its obligations under state and common laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised,

---

[15] See *supra* note 12.

lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

59. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

60. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

61. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

62. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

63. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices was inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

64. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

65. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff and Class Members as a result of the Data Breach.

Defendant Violated FTC Guidelines Prohibiting Unfair or Deceptive Acts

66. The Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") prohibits businesses from engaging in "unfair or deceptive acts or practices in or affecting commerce." The

FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

67. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[16]

68. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[17]

69. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

70. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

71. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

---

[16] See https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 7, 2024).

[17] See https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited October 7, 2024).

72. Defendant was at all times fully aware of its obligations to protect Plaintiff's and Class Members' Private Information because of its business model of collecting Private Information and storing such information. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant's Conduct Fails to Adhere to Industry Standards, HIPAA and HITECH Standards, and Commensurate Duties they Owed to Plaintiff and the Class

73. Defendant embraced a standard of care and commensurate duty defined by HIPAA, state law and common law to safeguard the PHI and PII of Plaintiff and Class Members.

74. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data under the condition and implied promise and assurance by Defendant that it would keep such Private Information confidential and secure. Accordingly, Defendant also had an implied duty to safeguard their data, independent of any statute.

75. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

76. On information and belief, Defendant is considered a Covered Entity, and/or in the alternative, a Business Associate pursuant to HIPAA.

77. Defendant is also regulated by the Health Information Technology Act ("HITECH"). See 42 U.S.C. §17921, 45 C.F.R. § 160.103.

78. Because Defendant is covered by HIPAA (45 C.F.R. § 160.102), it is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule

("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

79. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

80. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

81. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

82. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

83. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

84. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic

protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

85. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

86. Plaintiff's and Class Members' Personal and Medical Information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

87. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

88. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

89. Plaintiff's and Class Members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

90. Plaintiff's and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

91. Plaintiff's and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

92. Plaintiff's and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

93. Plaintiff's and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

94. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

95. HIPAA requires covered entities and business associates to protect against reasonably anticipated threats to the security of sensitive patient health information.

96. Covered entities and business associates must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

97. This Data Breach constitutes an unauthorized access of PHI, which is not permitted under the HIPAA Privacy Rule:

98. A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

99. The Data Breach could have been prevented if Defendant had implemented HIPAA mandated and industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its patients with respect to adequately securing and maintaining the confidentiality of Private Information.

100. It can be inferred from the Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Representative Plaintiff's and Class Members' PII and PHI.

101. Upon information and belief, prior to the Data Breach, Defendant was aware of its security failures but failed to correct them or adequately and timely disclose them to the public, including Plaintiff and Class Members.

102. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendant knew or should have known that it did not make such actions and failed to implement adequate data security practices.

103. Because Defendant failed to comply with industry standards, while monetary relief may cure some of Plaintiff's and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the PII and PHI of Plaintiff and Class Members; and without the supervision of the Court via injunctive relief, Plaintiff's and Class Members' PII and PHI remain at risk of subsequent Data Breaches.

104. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

105. Defendant owed a duty to Plaintiff and Class Members to ensure that the Private Information it collected and was responsible for was adequately secured and protected.

106. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

107. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach that impacted the Private Information it collected and was responsible for in a timely manner.

108. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

109. Defendant owed a duty to Plaintiff and Class Members to disclose if its data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust this Private Information to Defendant.

110. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

111. Defendant owed a duty to Plaintiff and Class Members to mitigate the harm suffered by the Representative Plaintiff's and Class Members' as a result of the Data Breach.

112. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system and safeguards to prevent data loss;
b. Failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach;
c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits;
d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights;
e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;
f. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information;
g. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information;

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons; and

i. Retaining information past a recognized purpose and not deleting it.

Value of the Relevant Sensitive Information

113. The high value of PII to criminals is evidenced by the prices they garner on the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[20]

114. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

115. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number,

---

[18] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited October 7, 2024).

[19] *Id*.

[20] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited October 7, 2024).

alien registration number, government passport number, employer or taxpayer identification number."

116. Identity thieves can use PII and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

117. The ramifications of Defendant's failure to keep secure Plaintiff's and Class Members' PII are long lasting and severe. Once PII and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII of Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

118. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

119. Data breaches are preventable.[22] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could

---

[21] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf (last visited October 7, 2024).

[22] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)

have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[23] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[24]

120. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[25]

Defendant's Delayed Response to the Breach

121. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII, especially their Social Security numbers, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Medicare numbers, Social Security numbers, Dates of birth, and other critical PII.

122. Despite this understanding, Defendant did not timely inform affected individuals, including Plaintiff and Class Members, about the Data Breach.

123. Defendant asserts that it first learned of the Data Breach on April 29, 2024. Despite possessing this knowledge, Defendant failed to act on it by immediately notifying Plaintiff and Class Members of the Data Breach.

---

23 *Id*. at 17.

24 *Id*. at 28.

25 *Id.*

124. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.6% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[26]

125. According to the U.S. Bureau of Labor Statistics' 2022 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[27] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[28] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

126. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

127. As a consequence of Defendant's inadequate data security systems and protection, Plaintiff and Class Members have been deprived of the benefit of their bargain which occurred when they agreed to receive services administered by Defendant. Plaintiff and Class Members, reasonable consumers – understandably expected that they were, in part, paying for the service and necessary data security to protect the Private Information when, in fact, Defendant had not provided the necessary adequate data security in any event. Consequently, Plaintiff and Class

---

[26] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2022/home.htm (__SMW CHECKlast visited July 24, 2024); see also U.S. BUREAU OF LABOR STATISTICS, Employment And Average Hourly Earnings By Industry, available at https://www.bls.gov/news.release/empsit.t19.htm (last visited July 24, 2024) (___SMW CHECKfinding that on average, private-sector workers make $1,166.20 per 40-hour work week).

[27] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html?&qsearchterm=James%20Wallman (last visited September 29, 2024).

[28] *Id.*

Members received services that were of a lesser value than what they had reasonably expected from and bargained for with Defendant.

CLASS ALLEGATIONS

128. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff asserts common law claims, as more fully alleged hereinafter, on behalf of the following Class.

> All individuals in the United States whose PHI/PII was accessed or otherwise compromised as a result of the Data Breach.

Members of the Class are referred to herein collectively as "Class Members" or "Class."

129. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

130. The proposed Class meets the requirements of Rule 23 of the Federal Rules of Civil Procedure, because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

131. **Numerosity**: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible.

132. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendant failed to adequately safeguard Plaintiff's and the Class Members' Private Information;

b) Whether Defendant failed to protect Plaintiff's and the Class Members'

Private Information, as promised;

c) Whether Defendant's computer system systems and data security practices used to protect Plaintiff's and the Class Members' Private Information violated federal, state, and local laws, or Defendant's duties;

d) Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and the Class Members' Private Information properly and/or as promised;

e) Whether Defendant violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, HIPAA, state privacy statutes, and/or FTC law or regulations, imposing duties upon Defendant, applicable to Plaintiff and Class Members;

f) Whether Defendant failed to notify Plaintiff and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendant acted negligently in failing to safeguard Plaintiff's and the Class Members' Private Information;

h) Whether Defendant entered into contracts that included contract terms requiring Defendant to protect the confidentiality of Plaintiff's Private Information and have reasonable security measures;

i) Whether Defendant's conduct described herein constitutes a breach of its contracts benefiting Plaintiff and each of the Class Members;

j) Whether Defendant should retain the money paid by Plaintiff and each of the Class Members to protect their Private Information;

k) Whether Plaintiff and the Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l) Whether Plaintiff and the Class Members are entitled to restitution as a result of Defendant's wrongful conduct;

m) What equitable relief is appropriate to redress Defendant's wrongful conduct; and

n) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class Members.

133. **Typicality**: Plaintiff's claims are typical of the claims of each of the Class Members. Plaintiff and the Class Members sustained damages as a result of Defendant's uniform wrongful conduct during transactions with them.

134. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiff. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and have the financial resources to do so. Neither Plaintiff nor her counsel have any interest adverse to those of the other members of the Class.

135. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendant or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendant still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PII of Plaintiff and Class Members.

136. **Class-wide Applicability**: This case is appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Plaintiff and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiff's challenge to those practices hinges on Defendant's conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

137. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendant's conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendant. Even if Class Members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

138. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

139. Plaintiff and Class Members were required to submit PII to Defendant, in order to obtain services.

140. Defendant knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII of Plaintiff and Class Members.

141. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose PII had been entrusted to Defendant.

142. Defendant breached its duty to Plaintiff and Class Members by failing to secure the PII that Defendant collected from consumers from unauthorized disclosure to third parties.

143. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' PII.

144. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because it collected and/or stored the PII of Plaintiff and the Class Members.

145. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

146. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duty. Defendant knew or should have known it was failing to meet its duty, and that Defendant's breach of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized exposure of their PII.

147. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

148. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

149. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Personal Information.

150. Defendant breached its duties to Plaintiff and Class Members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information, *i.e.,* by allowing Plaintiff's Private Information to be taken without Plaintiff's authorization by third parties.

151. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

152. But for Defendant's wrongful and negligent breach of its duty owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

153. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duty, and that Defendant's breach of that duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the unauthorized access to their PII.

154. On information and belief, as a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

155. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

156. Plaintiff and Class Members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendant, as alleged above.

157. The contracts respecting which Plaintiff and Class Members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendant would act fairly and in good faith in carrying out its contractual obligations to take reasonable measures to protect Plaintiff's PII from unauthorized disclosure and to comply with state laws and regulations.

158. A "special relationship" exists between Defendant and the Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members who

sought services from Defendant and, in doing so, entrusted Defendant, pursuant to its requirements and Privacy Notice, with their PII.

159. Despite this special relationship with Plaintiff, Defendant did not act in good faith and with fair dealing to protect Plaintiff's and Class Members' PII.

160. Plaintiff and Class Members performed all conditions, covenants, obligations, and promises owed to Defendant.

161. Defendant's failure to act in good faith in complying with the contracts denied Plaintiff and Class Members the full benefit of their bargain, and instead they received services that were less valuable than what they paid for and less valuable than their reasonable expectations.

162. Accordingly, on information and belief, Plaintiff and Class Members have been injured as a result of Defendant's breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Breach of Duty
(On Behalf of Plaintiff and the Class)

163. Plaintiff, on behalf of herself and the Class, re-alleges and incorporates the above allegations by reference.

164. Defendant accepted the special confidence placed in it by Plaintiff and Class Members. There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of their PII.

165. Defendant became the guardian of Plaintiff's and Class Members' PII and accepted a fiduciary duty to act primarily for the benefit of its patients, including Plaintiff and the Class Members, including safeguarding Plaintiff's and the Class Members' PII.

166. Defendant breached its fiduciary duty to Plaintiff and Class Members by (a) failing to protect the PII of Plaintiff and the Class; (b) by failing to notify Plaintiff and the Class Members

of the unauthorized disclosure of the PII; and (c) by otherwise failing to safeguard Plaintiff's and the Class Members' PII.

167. As a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiff and/or Class Members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiff's and Class Members' PII.

168. On information and belief, as a direct and proximate result of Defendant's breach of their fiduciary duty, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

169. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

170. Under Minn. Stat. § 555.01, this Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint, as Defendant's acts do here.

171. An actual controversy has arisen as a result of the Data Breach regarding Plaintiff's and Class Members' Private Information, and whether Defendant is currently maintaining sufficient data security measures to protect Plaintiff and the Class from further data breaches. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injuries as a result of the compromise of their Private Information and remain at imminent risk that further compromises will occur in the future.

172. Accordingly, Plaintiff requests that this Court, pursuant to its authority under Minn. Stat. § 555.01, should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure Private Information and to timely notify its patients, clients, customers or any individuals impacted of a data breach under the common law, Section 5 of the FTC act, and various state statutes; and

b. Defendant continues to breach its legal duty by failing to employ reasonable measures to secure customers' Private Information.

173. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect the Private Information that has been entrusted to it.

174. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach affecting Defendant's systems. The risk of another such breach is real, immediate, and substantial. If another breach of Defendant's system occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

175. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction were issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, any cost to Defendant for complying with an injunction would be minimal, and Defendant has a pre-existing legal obligation to employ such measures.

176. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach affecting Defendant's systems, thus preventing further injuries that would result to Plaintiff and Class Members, whose confidential information is already compromised.

COUNT VI
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

177. Plaintiff, on behalf of the Class, re-alleges and incorporates the above allegations by reference.

178. Defendant required Plaintiff and the Class to provide and entrust their PII/PHI as a condition of obtaining medical care and medical devices from Defendant.

179. Plaintiff and the Class paid money to Defendant in exchange for goods and services, as well as Defendant's promise or obligation to protect their protected health information and other PII from unauthorized disclosure.

180. Defendant promised and/or was bound by law to comply with HIPAA and HITECH standards and to make sure that Plaintiff's and Class Members' protected health information and other PII would remain protected.

181. Through its course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII/PHI and financial information.

182. Defendant required Plaintiff and Class Members to provide and entrust their PII/PHI, including for example, medical information, record or account numbers, names, and other information.

183. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII/PHI to Defendant, in exchange for, amongst other things, the protection of their PII/PHI. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

184. Plaintiff and the Class Members would not have entrusted their PII/PHI to Defendant in the absence of Defendant's implied promise to adequately safeguard this confidential personal and medical information.

185. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

186. Defendant breached the implied contracts it made with Plaintiff and the Class by making their PII/PHI accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII/PHI was secure, failing to encrypt Plaintiff and Class Members' sensitive PII/PHI, failing to safeguard and protect their medical, personal and financial information and by failing to provide timely and accurate notice to them that medical and personal information was compromised as a result of the data breach.

187. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to comply with its promise or obligation under the law to abide by HIPAA and HITECH.

188. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1).

189. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1).

190. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii).

191. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2).

192. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic protected

health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3).

193. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations in violation of 45 CFR 164.306(a)(94).

194. Defendant further breached its implied contracts with Plaintiff and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in compliance with 45 CFR 164.530(c).

195. Defendant further breached its implied contracts with Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII/PHI.

196. Defendant's failures to meet its promises and/or obligations constitute breaches of implied contracts.

197. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) and/or actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) and/or the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

198. As a result of Defendant's breach of implied contract, Plaintiff and the Class Members are entitled to and demand actual, consequential, and nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Class, prays for relief and judgment against Defendant as follows:

A. certifying the Class pursuant to Minnesota Rule of Civil Procedure 23, appointing Plaintiff as representative of the Class, and designating Plaintiff's counsel as Class Counsel;

B. declaring that Defendant's conduct violates the laws referenced herein;

C. finding in favor of Plaintiff and the Class on all counts asserted herein;

D. awarding Plaintiff and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiff and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiff and the Class punitive damages;

G. awarding Plaintiff and the Class civil penalties;

H. granting Plaintiff and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendant from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiff and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: October 8, 2024

Respectfully submitted,

/s/ Joel R. Rhine
Joel R. Rhine
NCSB 16028

Ruth Sheehan
NCSB 48069
Rhine Law Firm, P.C.
North Carolina State Bar No. 16028
1612 Military Cutoff, Suite 300
Wilmington, NC 28403
Telephone : (910) 772-9960
Facsimile: (910) 772-9062
jrr@rhinelawfirm.com
ras@rhinelawfirm.com

/s/ Stephen R. Basser
Stephen R. Basser*
Samuel M. Ward*
Barrack, Rodos & Bacine
600 Broadway # 900
San Diego, CA 92101
Telephone: (619) 230-0800
sbasser@barrack.com
sward@barrack.com

and

Jordan R. Laporta*
Barrack, Rodos & Bacine
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
Telephone: (215) 963-0600
jlaporta@barrack.com

Counsel for Plaintiff

*Application for admission *Pro Hac Vice* to be filed